
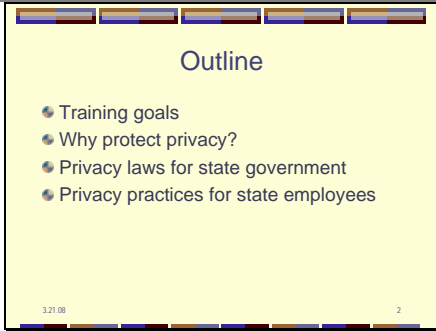
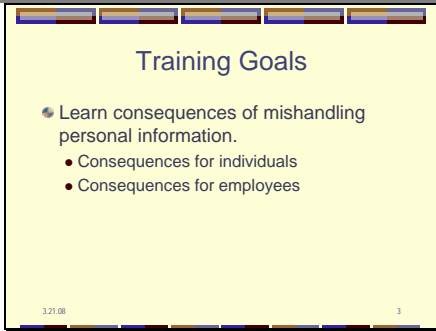


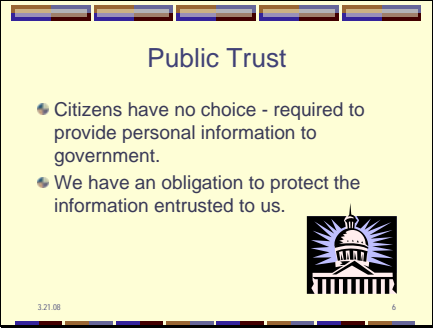
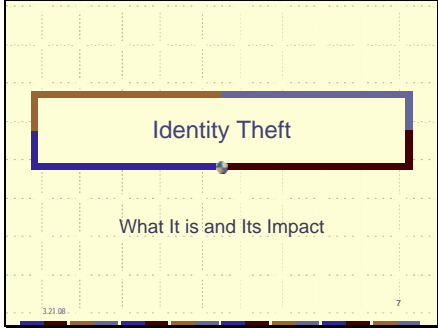
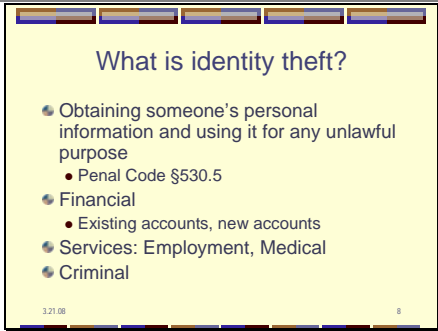


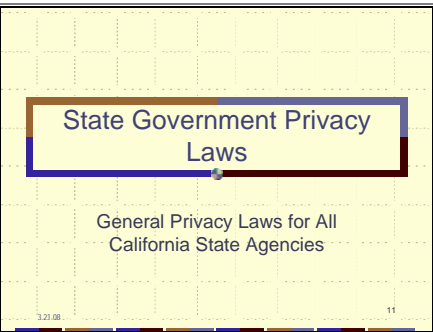


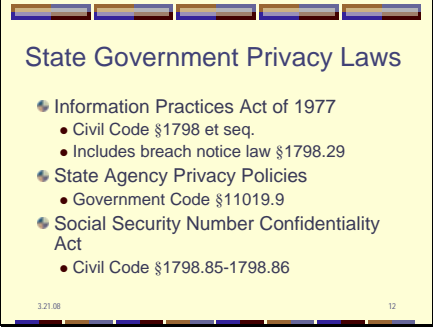
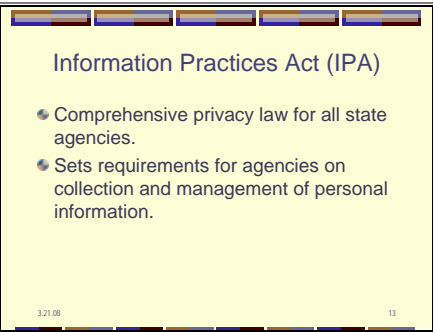
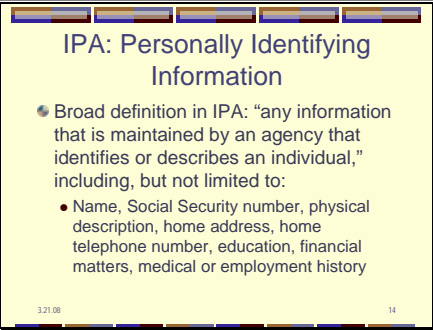
## Basic State Employee Privacy Training with Speaker Notes

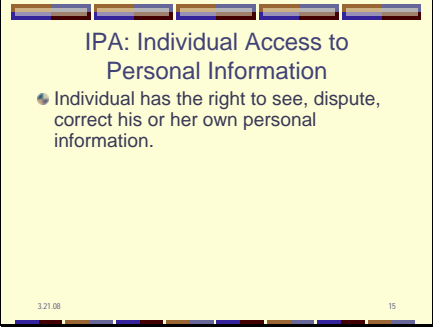
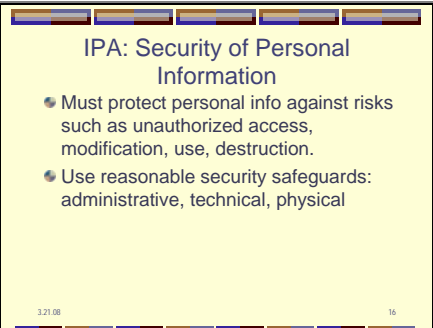
Slide 1		
Slide 2		
Slide 3		<p>This training is intend to make employees aware of the consequences of mishandling personal information –</p> <ul style="list-style-type: none"><li>▪ consequences for the individuals whose info is mishandled</li><li>▪ consequences for state employees</li></ul>

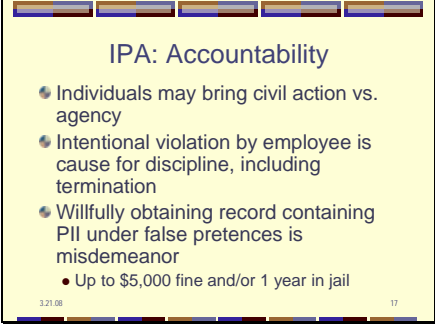
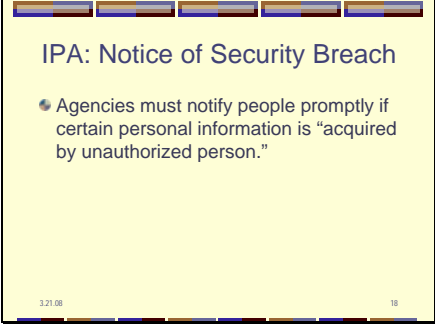
Slide 4	 <p><b>Training Goals</b></p> <ul style="list-style-type: none"> <li>Learn risky information-handling practices to avoid. <ul style="list-style-type: none"> <li>Recognize other such practices in your workplace.</li> </ul> </li> <li>Learn when and how to report information security incidents.</li> </ul> <p>3.21.08 4</p>	<p>The training will make you aware of some dangerous information-handling practices - and help you to recognize other risky practices in your workplace.</p> <p>You will also learn when and how to report information security incidents in your workplace.</p>
Slide 5	 <p><b>Why protect privacy?</b></p> <ul style="list-style-type: none"> <li>It's the law! <ul style="list-style-type: none"> <li>Information Practices Act, and others</li> </ul> </li> <li>Security breaches <ul style="list-style-type: none"> <li>Notifying affected individuals can cost over \$200 per notice.</li> </ul> </li> <li>Identity theft <ul style="list-style-type: none"> <li>The low-risk, high-reward crime of our times</li> </ul> </li> </ul> <p>3.21.08 5</p>	<p>Law – State laws require state agencies to protect personal information</p> <p>Security breaches – for example, lost laptops containing personal information – cost state agencies <b>money</b> (notifying all affected parties) and loss of <b>reputation and trust</b> of citizens.</p> <ul style="list-style-type: none"> <li>Source: Ponemon Institute study of data breach cost (3/2011).</li> </ul> <p>Identity theft – Personal information is sought by identity thieves, who use it to harm people.</p>
Slide 6	 <p><b>Public Trust</b></p> <ul style="list-style-type: none"> <li>Citizens have no choice - required to provide personal information to government.</li> <li>We have an obligation to protect the information entrusted to us.</li> </ul> <p>3.21.08 6</p>	<p>People can't go to another DMV, another FTB, if they're not happy with the way their personal information is handled.</p> <p>People entrust their most sensitive personal information – financial information, medical information – to Government agencies.</p> <p>Our failure to protect personal information and use it properly can undermine Californians' faith in their government.</p>

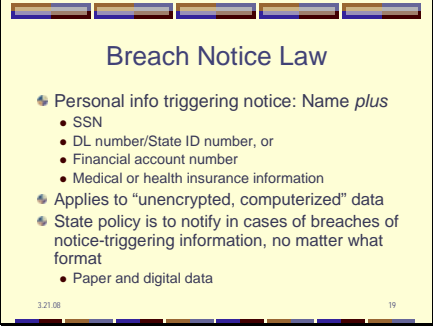

Slide 7		
Slide 8		<p>The most common type of identity theft is financial – thieves steal personal information and use it to make money.</p> <p>A thief may use a victim’s existing account – such as a credit card account. Or a thief may use personal information such as name and Social Security number to open new accounts.</p> <p>Other kinds of identity theft include using someone’s SSN to get a <u>job</u> – which can create tax liabilities for the victim.</p> <p>Or a thief may use someone’s information to get <u>medical benefits</u> – which can cost the victim’s insurer. This can also pollute the victim’s medical records with the thief’s diagnoses and treatments, putting the victim’s health at risk.</p> <p><u>“Criminal” identity theft</u> is when a thief uses someone’s information when arrested or charged with a crime, which creates a criminal record for the victim. This can be very difficult to correct.</p>

<p>Slide 9</p>	 <p><b>Incidence of Identity Theft</b></p> <ul style="list-style-type: none"> <li>8.1 million in 2010</li> <li>3.5% of adults</li> <li>Including 1 million Californians</li> </ul>	<p>According to the most recent nationwide survey, there were 9.9 million identity theft victims in 2008.</p> <ul style="list-style-type: none"> <li>Javelin Strategy &amp; Research, published 2/09</li> </ul> <p>About 1 million of them were Californians.</p>
<p>Slide 10</p>	 <p><b>Impact of ID Theft on Economy</b></p> <ul style="list-style-type: none"> <li>Total cost of identity theft in U.S. in 2010</li> </ul> <p><b>\$37 Billion</b></p>	<p>\$37billion was the total cost to the economy. About \$5 billion of that was victim costs. The rest – \$32 billion – was the cost to financial institutions and merchants.</p> <p>Of course, it's ultimately consumers who pay those costs, through higher prices for goods and services.</p>
<p>Slide 11</p>	 <p><b>State Government Privacy Laws</b></p> <p>General Privacy Laws for All California State Agencies</p>	

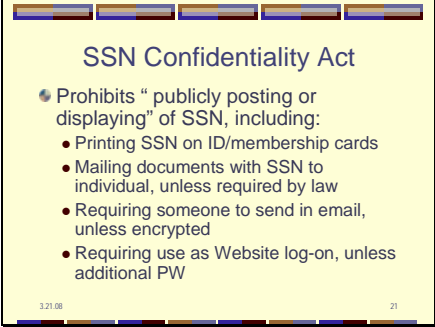

<p>Slide 12</p>	 <p><b>State Government Privacy Laws</b></p> <ul style="list-style-type: none"> <li>Information Practices Act of 1977 <ul style="list-style-type: none"> <li>Civil Code §1798 et seq.</li> <li>Includes breach notice law §1798.29</li> </ul> </li> <li>State Agency Privacy Policies <ul style="list-style-type: none"> <li>Government Code §11019.9</li> </ul> </li> <li>Social Security Number Confidentiality Act <ul style="list-style-type: none"> <li>Civil Code §1798.85-1798.86</li> </ul> </li> </ul> <p>3.21.08 12</p>	<p>In addition to these laws, which apply to all state agencies, there are also state laws protecting specific kinds of personal information (such as HIV diagnoses, driver license info) and federal laws applying to certain state agencies.</p>
<p>Slide 13</p>	 <p><b>Information Practices Act (IPA)</b></p> <ul style="list-style-type: none"> <li>Comprehensive privacy law for all state agencies.</li> <li>Sets requirements for agencies on collection and management of personal information.</li> </ul> <p>3.21.08 13</p>	
<p>Slide 14</p>	 <p><b>IPA: Personally Identifying Information</b></p> <ul style="list-style-type: none"> <li>Broad definition in IPA: "any information that is maintained by an agency that identifies or describes an individual," including, but not limited to: <ul style="list-style-type: none"> <li>Name, Social Security number, physical description, home address, home telephone number, education, financial matters, medical or employment history</li> </ul> </li> </ul> <p>3.21.08 14</p>	<p><b>Information Practices Act (Civil Code §1798.3)</b></p> <p>The IPA uses a very broad definition of personal information – not just the very sensitive type such as medical, financial, SSN, the kind that ID thieves are after – but also home address &amp; phone number, education, etc.</p>

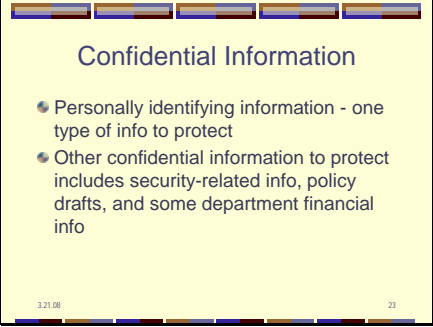
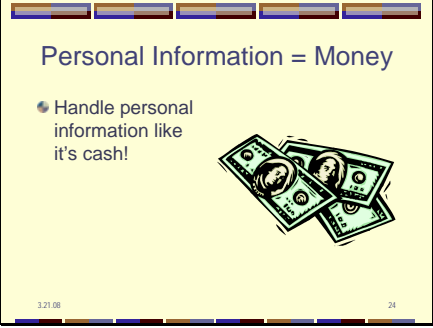
<p>Slide 15</p>		<p>IPA (Civil Code §§1798.30-1798.44)</p> <p>We all have the right, under the Information Practices Act, to see the records government maintains on us – and the right to dispute, and correct our records if in error.</p>
<p>Slide 16</p>		<p>IPA (Civil Code §1798.20-1798.21)</p> <p>The IPA requires state agencies to protect personal information from unauthorized, access, use, modification, destruction, etc.</p> <p>Agencies must use reasonable and appropriate safeguards to protect personal information.</p> <p>Administrative safeguards – such as policies on use of passwords for access to databases</p> <p>Technical safeguards – such as firewalls and encryption of data</p> <p>Physical safeguards – such as locked file cabinets, buildings with card key-controlled access</p> <p>We'll cover some other examples of practices for safeguarding personal information later on in the class.</p>

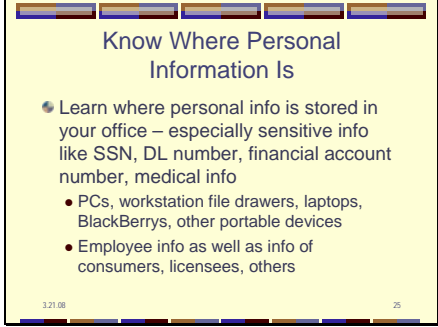
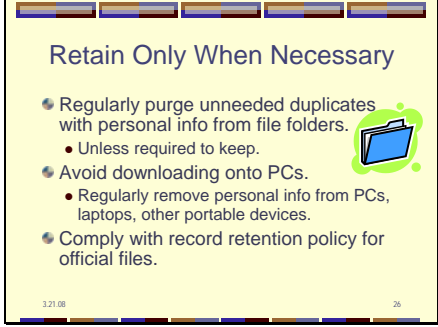
<p>Slide 17</p>	 <p><b>IPA: Accountability</b></p> <ul style="list-style-type: none"> <li>• Individuals may bring civil action vs. agency</li> <li>• Intentional violation by employee is cause for discipline, including termination</li> <li>• Willfully obtaining record containing PII under false pretences is misdemeanor <ul style="list-style-type: none"> <li>• Up to \$5,000 fine and/or 1 year in jail</li> </ul> </li> </ul>	<p>Civil Code § 1798.45-1798.57</p> <p>There are <i>consequences</i> for violating the Information Practices Act.</p> <p>Consequences for an agency – which may be sued, if violation results in adverse impact.</p> <p>Consequences for an employee – if the violation is intentional.</p> <p>Also consequences for an employee who obtains personal information under false pretences – Misdemeanor, punishable by a fine of up to \$5,000 and one year in jail.</p>
<p>Slide 18</p>	 <p><b>IPA: Notice of Security Breach</b></p> <ul style="list-style-type: none"> <li>• Agencies must notify people promptly if certain personal information is “acquired by unauthorized person.”</li> </ul>	<p>Breach Notice Law is part of Information Practices Act for State agencies §1798.29 – (Also applies to businesses, Civil Code §1798.82).</p> <p>Requires notification of individuals if their personal information – of a specific type – is “acquired by an unauthorized person” – or is reasonably believed to have been acquired.</p> <p>Intent of law is to give people early warning when their personal info has been compromised – to give them opportunity to take steps to protect themselves against ID theft.</p> <p>For example, if your SSN is involved in a breach, you can place a fraud alert or security freeze on your credit files, protecting you from new accounts being opened using your information.</p>

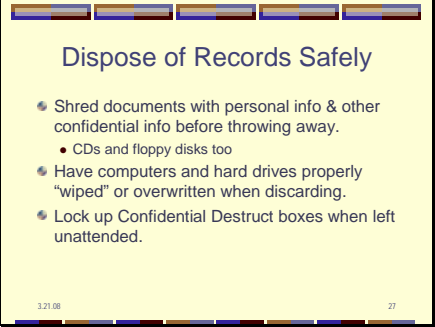

<p>Slide 19</p>		<p>Generally, the kind of personal information that triggers the notice requirement is the kind identity thieves want.</p> <p>Financial account number: for example bank account number, credit card or debit card number – with PIN if required for access to account.</p> <p>Requirement to notify applies to “unencrypted, computerized” data.</p> <ul style="list-style-type: none"> <li>• Encrypted means coded or scrambled so that it’s not readable except by those who have a key.</li> </ul> <p>State policy for state agencies is to notify in case of breaches involving “notice-triggering” personal information – <u>in any format – paper, electronic, tape, etc.</u></p> <ul style="list-style-type: none"> <li>• Risk to individuals is same, whether their data was on paper in a manila folder or in a database on a computer.</li> <li>• Authority: Management Memo 06-12: Protection of Information Assets</li> </ul>
<p>Slide 20</p>		<p>Records can be public – but personal information in the records is still protected – which is why state agencies redact (black out) personal information.</p> <p>Check with your department’s Public Records Act coordinator or Legal office if you have questions.</p>

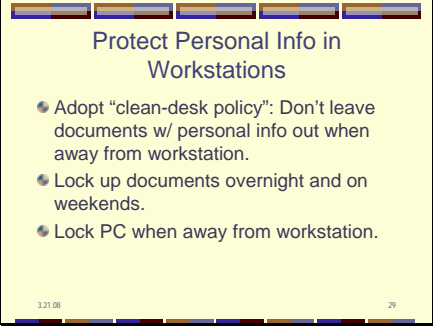
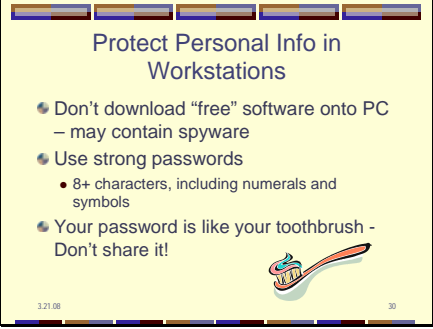


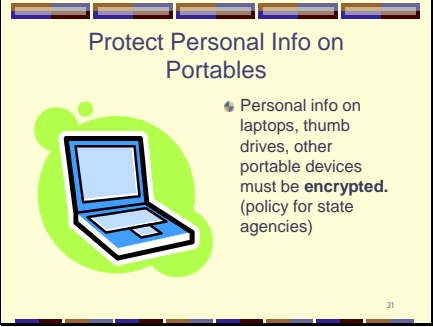
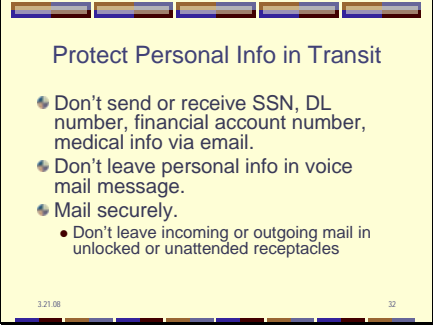
<p>Slide 21</p>	 <p><b>SSN Confidentiality Act</b></p> <ul style="list-style-type: none"> <li>Prohibits “publicly posting or displaying” of SSN, including: <ul style="list-style-type: none"> <li>Printing SSN on ID/membership cards</li> <li>Mailing documents with SSN to individual, unless required by law</li> <li>Requiring someone to send in email, unless encrypted</li> <li>Requiring use as Website log-on, unless additional PW</li> </ul> </li> </ul>	<p><b>Social Security Number Confidentiality Act (Civil Code §1798.85-1798.86)</b></p> <ul style="list-style-type: none"> <li>Applies to any person or entity – therefore to state gov’t, local gov’t, private sector.</li> <li>Prohibits public posting or display of SSNs</li> <li>Doesn’t prohibit internal use for administrative purposes.</li> <li>Also specifically prohibits certain types of public posting – such as printing on ID card for access to goods or services <ul style="list-style-type: none"> <li>This is why our health plan cards no longer have our SSNs on them.</li> </ul> </li> </ul>
<p>Slide 22</p>	 <p><b>Recommended Privacy Practices</b></p> <p>Basic Practices for State Employees</p>	<p>The following are some <u>basic practices for handling personal information responsibly</u>, so that it is protected from unauthorized access and use.</p> <p>These practices are appropriate for most – but not all – work environments. They are intended to make you aware of safer – and of less safe – ways to handle the personal information that you come into contact with in your job.</p> <p>If you have questions about the applicability of any of these recommended practices in your workplace, please raise the issue with your supervisor or with your department’s Information Security or Privacy Officer.</p>

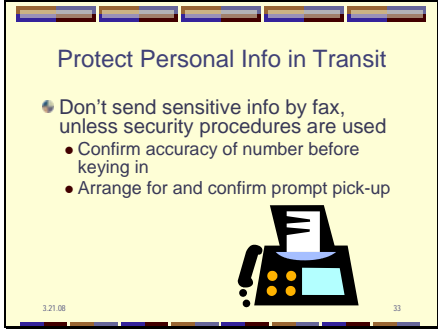

<p>Slide 23</p>	 <p><b>Confidential Information</b></p> <ul style="list-style-type: none"> <li>● Personally identifying information - one type of info to protect</li> <li>● Other confidential information to protect includes security-related info, policy drafts, and some department financial info</li> </ul> <p>3.21.08 23</p>	<p>Protecting personal identifying information (PII) protects individuals' privacy.</p> <p>Agencies must also protect other kinds of confidential information – such as computer security information and department banking information.</p> <p>Practices described here are intended to protect personal information – but they would also protect other kinds of confidential state information.</p>
<p>Slide 24</p>	 <p><b>Personal Information = Money</b></p> <ul style="list-style-type: none"> <li>● Handle personal information like it's cash!</li> </ul> <p>3.21.08 24</p>	<p>Personal information is worth money – There's a black market for personal information and identity thieves use it to make money.</p> <p>If you thought of personal information as cash, you would probably handle it differently.</p> <p>You wouldn't leave a pile of \$100 bills lying on your desk when you're away even just for a short meeting, for example.</p> <p>This is how we should all think of the personal information in our care.</p>

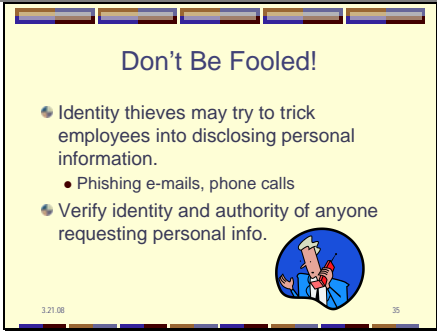
<p>Slide 25</p>	 <p><b>Know Where Personal Information Is</b></p> <ul style="list-style-type: none"> <li>Learn where personal info is stored in your office – especially sensitive info like SSN, DL number, financial account number, medical info <ul style="list-style-type: none"> <li>PCs, workstation file drawers, laptops, BlackBerrys, other portable devices</li> <li>Employee info as well as info of consumers, licensees, others</li> </ul> </li> </ul>	<p>Do you store downloaded personal information on your PC?</p> <p>Do you have print-outs of personal information in file folders in an unlocked drawer in your workstation?</p> <p>Do you have CDs or floppy disks with files on them containing personal information?</p> <p>The first step to protecting personal information is to know where it is. Take a look around your workstation – in your desk drawers, file drawers, shelves – see where you have personal information stored.</p>
<p>Slide 26</p>	 <p><b>Retain Only When Necessary</b></p> <ul style="list-style-type: none"> <li>Regularly purge unneeded duplicates with personal info from file folders. <ul style="list-style-type: none"> <li>Unless required to keep.</li> </ul> </li> <li>Avoid downloading onto PCs. <ul style="list-style-type: none"> <li>Regularly remove personal info from PCs, laptops, other portable devices.</li> </ul> </li> <li>Comply with record retention policy for official files.</li> </ul>	<p>When you've started to locate where you're keeping personal information in your workstation – consider whether you really need to keep it all.</p> <p>There are some kinds of records and data that we're required to keep, for legal reasons.</p> <p>But there are probably lots of other files – paper and digital – that we no longer need, don't need to keep – and <b>SHOULD NOT</b> keep beyond the period when we're working on them.</p> <p>Develop the habit of regularly purging documents containing personal information from your file folders.</p> <p>Avoid downloading from databases onto your PC – regularly delete what you do download when you've finished using it.</p>

<p>Slide 27</p>	 <p><b>Dispose of Records Safely</b></p> <ul style="list-style-type: none"> <li>Shred documents with personal info &amp; other confidential info before throwing away. <ul style="list-style-type: none"> <li>CDs and floppy disks too</li> </ul> </li> <li>Have computers and hard drives properly "wiped" or overwritten when discarding.</li> <li>Lock up Confidential Destruct boxes when left unattended.</li> </ul> <p>3.21.08 27</p>	<p>Don't throw documents containing personal information into your waste basket or recycling bin – shred them first.</p> <p>CDs and floppy disks can also be shredded too.</p> <ul style="list-style-type: none"> <li>Consult your department's Information Security Officer about disposing of other data storage media.</li> </ul> <p>Or use your office's Confidential Destruct boxes for large quantities of sensitive documents.</p> <p>And manage Confidential Destruct boxes securely – They're effectively labeled "Here's the good stuff – take this first!"</p> <ul style="list-style-type: none"> <li>Don't leave Confidential Destruct boxes unattended during the day - Lock them up over night.</li> </ul>
<p>Slide 28</p>	 <p><b>Protect Personal Info from Unauthorized Access</b></p> <ul style="list-style-type: none"> <li>Limit access to personal info to those who need to use it to perform their duties. <ul style="list-style-type: none"> <li>Minimum necessary access</li> </ul> </li> </ul> <p>3.21.08 28</p>	<p>Not everyone in an office NEEDS to have access to all files and databases containing personal information.</p> <p>Especially info like SSN, DL number, financial account number, medical info.</p> <p>Don't give your access to co-workers or others who are not authorized.</p>



<p>Slide 29</p>		<p>Remember to treat personal information like cash – don't leave it sitting out on your desk when you're away.</p> <p>Put files and disks containing personal info in locked drawers or cabinets overnight.</p> <p>Lock your PC – Remember “Control, alt, delete before you leave your seat.”</p>
<p>Slide 30</p>		<p>Free software may not be free – It may contain spyware that can</p> <ul style="list-style-type: none"> <li>• impair the operation of your computer,</li> <li>• carry malicious programs that can steal your passwords and data,</li> <li>• introduce a virus into your department's system.</li> </ul> <p>Check with your IT department before loading any software you think you need.</p> <p>Don't use obvious facts or numbers as your password – not spouse's or child's name, not birth date.</p> <ul style="list-style-type: none"> <li>• Use combination of numbers, letters, symbols – 8+ characters</li> <li>• One way to create a memorable password that others can't guess is to use initial letters of a sentence that has meaning to you – substituting numbers for some letters and adding symbols. <ul style="list-style-type: none"> <li>• My favorite color is purple = mfc1p&amp;</li> </ul> </li> </ul> <p>Don't leave your password posted on your PC, don't share it with others.</p>

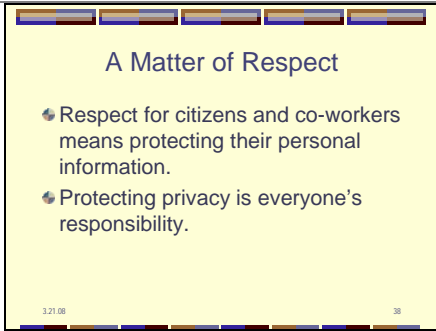

<p>Slide 31</p>		<p>It's now policy for state government agencies that personal information (especially SSNs, DL/ID numbers, financial account number, medical info) on laptop or other portable computing device or storage device like CD or thumb drive – <b>MUST BE ENCRYPTED.</b></p> <p><b>Authority: SAM 5345.2</b></p> <p>Many of the security breaches requiring notification in recent years have involved lost or stolen laptops or other portable devices.</p> <p>When personal information on portable devices is encrypted, it <b>can't</b> be accessed or used by an unauthorized person.</p>
<p>Slide 32</p>		<p>Think of email as a post card – Don't send personal information or other sensitive information by email – It's not a secure medium. Easy to send to wrong people.</p> <ul style="list-style-type: none"> <li>• There are procedures for encrypting email. Consult your Information Security Officer.</li> </ul> <p>Don't leave personal information in a voice mail message – you don't know who might pick up the message.</p> <ul style="list-style-type: none"> <li>• <u>Example</u>: Messages from doctor's office left on voice mail of state employee with phone number similar to a pharmacy. Messages contained confidential information.</li> </ul> <p>Mail thieves are often after personal information. Don't leave outgoing mail</p>

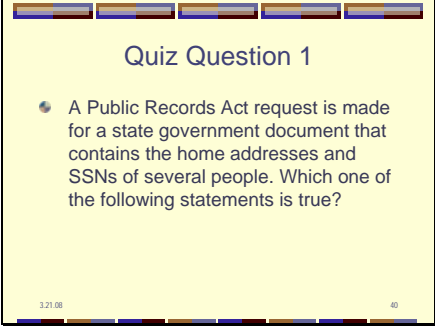
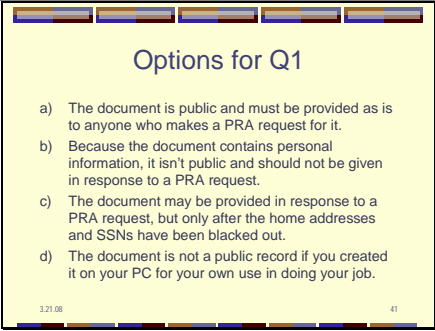
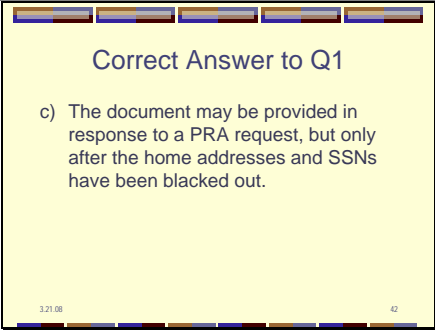
		<p>unattended – lock it away when leaving the area. Same for incoming mail.</p> <ul style="list-style-type: none"> <li>• <u>Example</u>: Theft of mail delivered to a department on Saturday. Contained documents with SSNs and checks. Required mass notification via news media and Web site because not known whose mail was stolen, individual notice not possible.</li> </ul>
Slide 33		<p>Fax also insecure – don't know who will see or pick up fax from machine. Also easy to mis-key and send to wrong person.</p> <p>If you must fax personal information, use special procedures.</p> <ul style="list-style-type: none"> <li>• Confirm number and key in carefully</li> <li>• Call recipient to notify of fax and get confirmation of prompt pick-up.</li> </ul>
Slide 34		<p>Unless you are authorized by your supervisor or manager, don't take or send State records containing personal information home.</p> <p>If you are authorized to work on state records at home, do so only on State computer equipment.</p> <ul style="list-style-type: none"> <li>• Home computer may not have appropriate security protections. And may be used by others who are not authorized to see state records.</li> </ul> <p>Consider recent events when federal VA employee took home a computer containing personal info on 26 million veterans, Home broken into and</p>

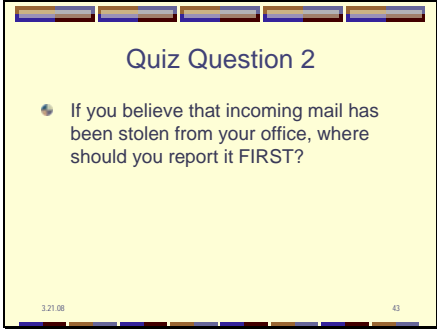
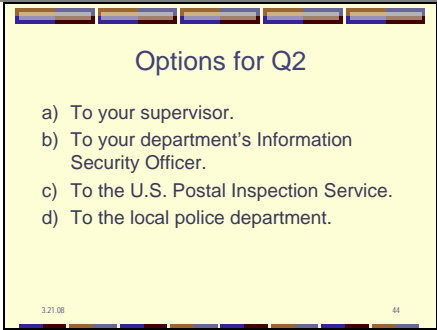
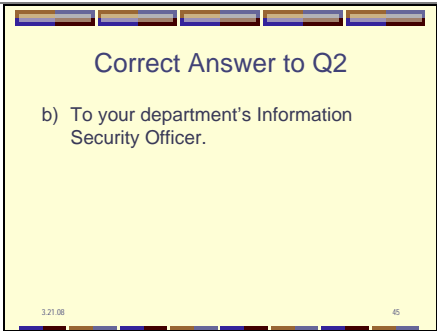
		<p>computer stolen.</p> <ul style="list-style-type: none"> <li>• Resulted in notification and anxiety for millions of veterans, other service personnel.</li> <li>• Many congressional hearings, several VA employees lost jobs.</li> </ul>
Slide 35		<p>Identity thieves often try to steal confidential information by lying and manipulating someone into providing it.</p> <p>One common form is what's known as "phishing" – an email that looks like it's from a bank or a government agency, for example, asking you to confirm your password, account number, or Social Security number – claiming to part of an effort to protect you from fraud.</p> <ul style="list-style-type: none"> <li>• The advice to consumers in light of phishing – which takes place over the phone as well as by email – is <b>NEVER</b> give out your personal information unless you initiated the contact.</li> </ul> <p>Such schemes are also targeted at businesses and gov't agencies – relying on workers' desire to provide good customer service.</p> <ul style="list-style-type: none"> <li>• When you get a request for personal information on individuals from someone you don't know, make an effort to verify the identity and authority of the requester.</li> <li>• If you're not sure, check with your supervisor.</li> </ul>

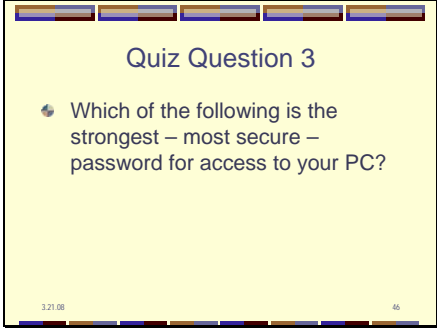
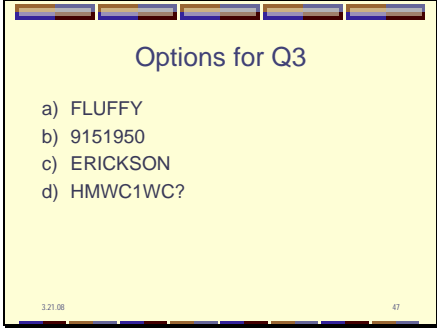
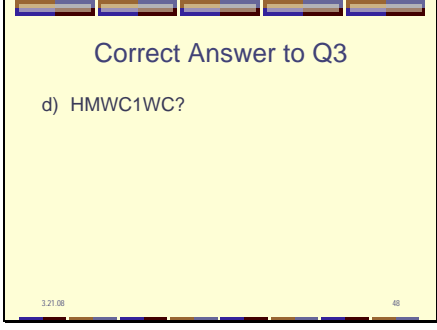


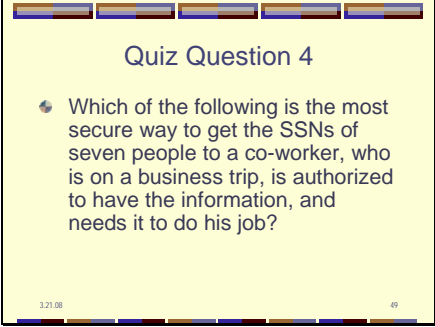
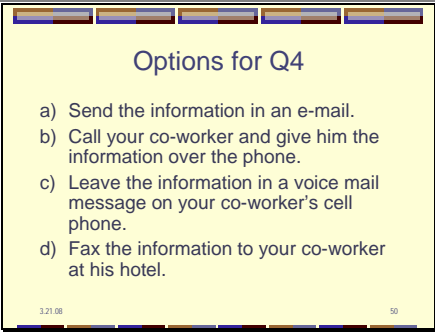
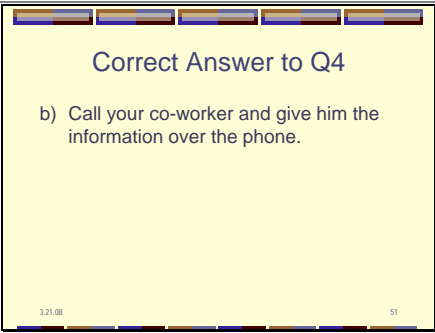
<p>Slide 36</p>		<p>In order to be able to maintain good information security – to protect the information people give to us – departments must know about and report information security incidents promptly.</p> <p>Be alert to incidents that could expose information to unauthorized access, disclosure, modification, or destruction.</p> <p>Such an incident could be</p> <ul style="list-style-type: none"> <li>• Lost or stolen computer, PDA, CD</li> <li>• Lost or stolen mail containing documents or other records</li> <li>• Improperly disposed of documents</li> <li>• An unauthorized person getting access to information</li> <li>• A virus interfering with operation of your computer</li> </ul> <p>[Next slide is about reporting incidents.]</p>
<p>Slide 37</p>		<p><b>[Fill in with phone number and email address of your department's Information Security Office.]</b></p> <p>Report any information security incident <b>PROMPTLY</b> to your department's Information Security Office.</p> <ul style="list-style-type: none"> <li>• Even if you're not sure an incident involves personal information.</li> <li>• Your ISO will determine the extent and significance of the incident.</li> </ul> <p>Of course, report the incident to your supervisor or manager.</p> <p>Over-report, rather than under-report,</p>

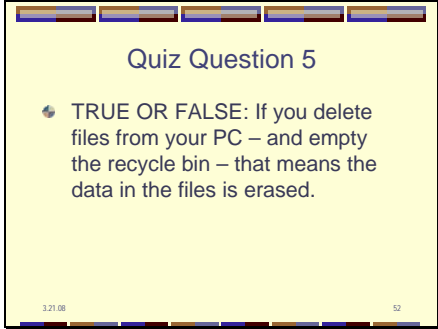
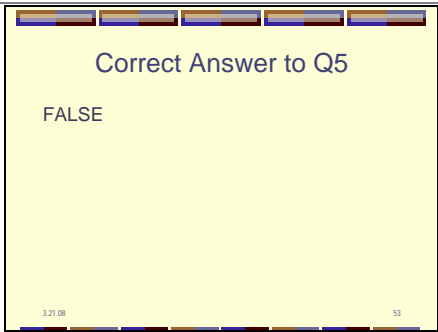
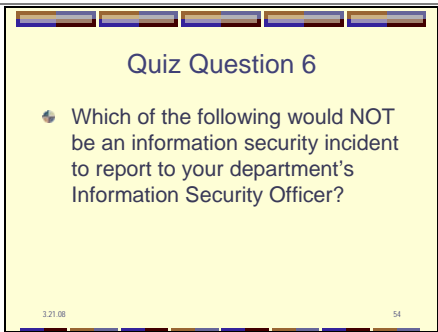
		<p>potential incidents.</p> <p>And prompt reporting is essential.</p> <ul style="list-style-type: none"> <li>• The sooner an incident can be investigated, the sooner any security holes can be filled.</li> </ul>
Slide 38		<p>Protecting privacy is a matter of respect:</p> <ul style="list-style-type: none"> <li>• Respect for our fellow citizens who entrust us with their personal information, and</li> <li>• Respect for our co-workers, whose information is also in our department's care.</li> </ul> <p>Protecting personal information is something an Information Security Officer or a Privacy Officer can do alone. We all touch some of the personal information in our offices and we are all responsible for protecting it.</p>
Slide 39		

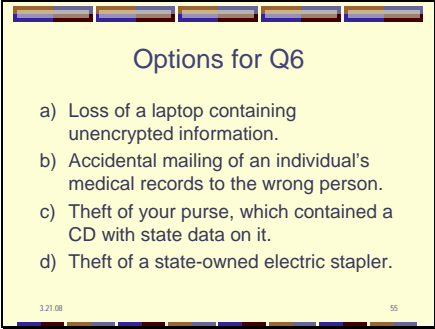
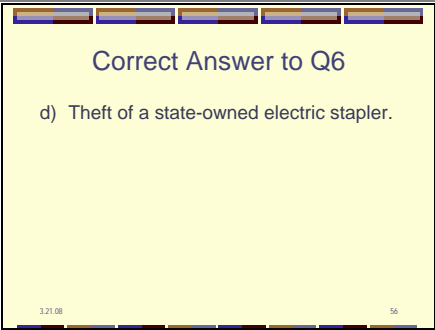
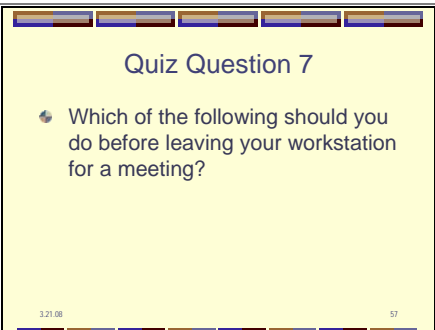
<p>Slide 40</p>	 <p>Quiz Question 1</p> <p>A Public Records Act request is made for a state government document that contains the home addresses and SSNs of several people. Which one of the following statements is true?</p> <p>3.21.08 40</p>	
<p>Slide 41</p>	 <p>Options for Q1</p> <ul style="list-style-type: none"> <li>a) The document is public and must be provided as is to anyone who makes a PRA request for it.</li> <li>b) Because the document contains personal information, it isn't public and should not be given in response to a PRA request.</li> <li>c) The document may be provided in response to a PRA request, but only after the home addresses and SSNs have been blacked out.</li> <li>d) The document is not a public record if you created it on your PC for your own use in doing your job.</li> </ul> <p>3.21.08 41</p>	
<p>Slide 42</p>	 <p>Correct Answer to Q1</p> <ul style="list-style-type: none"> <li>c) The document may be provided in response to a PRA request, but only after the home addresses and SSNs have been blacked out.</li> </ul> <p>3.21.08 42</p>	<p>c) The document may be provided in response to a PRA request, but only after the home addresses and Social Security numbers have been blacked out.</p> <p>Check with your supervisor or your department's PRA Coordinator on any PRA request.</p> <p>The requirements of the Public Records Act and the Information Practices Act must often be balanced. Redacting or blacking out personal information in public records is one way to do this.</p> <p>Note that the fact that you created the document for your own use in doing your job does NOT prevent it from being a public record.</p> <p>Government Code §6252 (e) "Public</p>

		records” includes any writing containing information relating to the conduct of the public’s business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.
Slide 43	 <p>Quiz Question 2</p> <p>● If you believe that incoming mail has been stolen from your office, where should you report it FIRST?</p> <p>3.21.08 43</p>	
Slide 44	 <p>Options for Q2</p> <ul style="list-style-type: none"> <li>a) To your supervisor.</li> <li>b) To your department's Information Security Officer.</li> <li>c) To the U.S. Postal Inspection Service.</li> <li>d) To the local police department.</li> </ul> <p>3.21.08 44</p>	
Slide 45	 <p>Correct Answer to Q2</p> <p>b) To your department's Information Security Officer.</p> <p>3.21.08 45</p>	<p>b) To your department’s Information Security Officer.</p> <p>You should also report the mail theft to your supervisor. But in order to ensure that a possible security breach is handled promptly, let your ISO know about any information security incident as soon as you discover it.</p>

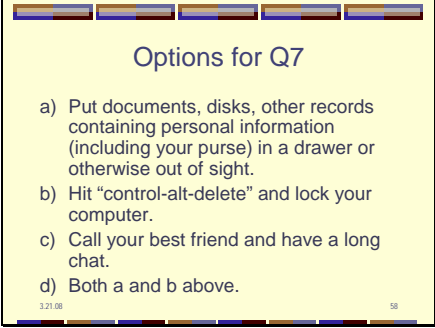
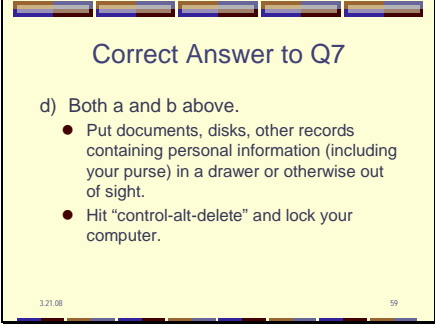
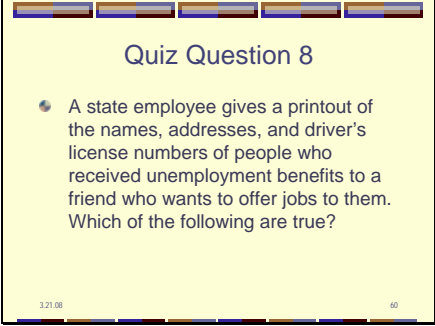
<p>Slide 46</p>	 <p>Quiz Question 3</p> <p>Which of the following is the strongest – most secure – password for access to your PC?</p> <p>3.21.08 46</p>	
<p>Slide 47</p>	 <p>Options for Q3</p> <ul style="list-style-type: none"> <li>a) FLUFFY</li> <li>b) 9151950</li> <li>c) ERICKSON</li> <li>d) HMWC1WC?</li> </ul> <p>3.21.08 47</p>	
<p>Slide 48</p>	 <p>Correct Answer to Q3</p> <p>d) HMWC1WC?</p> <p>3.21.08 48</p>	<p>d) HMWC1WC?</p> <p>A strong password contains at least 8 characters, including numbers and symbols. Weak, i.e. easy to guess, passwords include pet names, birth dates or anniversaries, and your mother's maiden name. This one is based on the first letters of the words in the sentence "How much wood could a woodchuck chuck?" It's something you can remember but it's difficult for others to guess.</p>

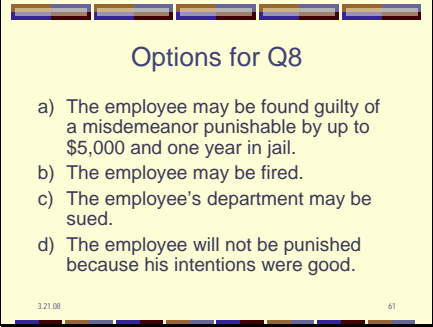
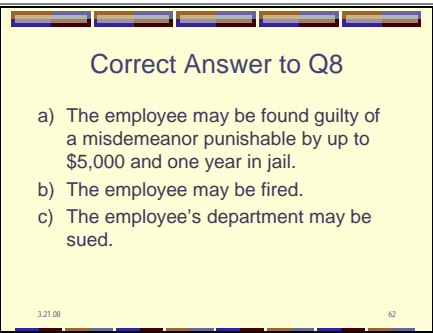
<p>Slide 49</p>		
<p>Slide 50</p>		
<p>Slide 51</p>		<p>b) Call your co-worker and give him the information over the phone.</p> <p>Calling your co-worker is the best of the alternatives. Email is not a secure communications channel, because it can be hacked into as it passes over the Internet. Voice mail is generally not secure because other people may pick up the message. Faxes, especially to a public fax machine like a hotel's, are also not secure. Note that the employee is authorized to have this information, which is the first issue to consider.</p>

<p>Slide 52</p>	 <p>Quiz Question 5</p> <p>TRUE OR FALSE: If you delete files from your PC – and empty the recycle bin – that means the data in the files is erased.</p> <p>3.21.08 52</p>	
<p>Slide 53</p>	 <p>Correct Answer to Q5</p> <p>FALSE</p> <p>3.21.08 53</p>	<p><b>FALSE</b></p> <p>Erasing data from a computer does not completely remove it. Special overwriting software must be used to properly “wipe” a hard drive. Check with your Information Security Officer before disposing of any computer hardware.</p>
<p>Slide 54</p>	 <p>Quiz Question 6</p> <p>Which of the following would NOT be an information security incident to report to your department's Information Security Officer?</p> <p>3.21.08 54</p>	

<p>Slide 55</p>	 <p>Options for Q6</p> <ul style="list-style-type: none"> <li>a) Loss of a laptop containing unencrypted information.</li> <li>b) Accidental mailing of an individual's medical records to the wrong person.</li> <li>c) Theft of your purse, which contained a CD with state data on it.</li> <li>d) Theft of a state-owned electric stapler.</li> </ul> <p>3.21.08 55</p>	
<p>Slide 56</p>	 <p>Correct Answer to Q6</p> <p>d) Theft of a state-owned electric stapler.</p> <p>3.21.08 56</p>	<p>d) Theft of a State-owned electric stapler.</p> <p>All of the other incidents involve data, which may include personal information or other confidential information. The theft of the stapler should be reported to your supervisor as a theft of state equipment.</p>
<p>Slide 57</p>	 <p>Quiz Question 7</p> <p>Which of the following should you do before leaving your workstation for a meeting?</p> <p>3.21.08 57</p>	



<p>Slide 58</p>	 <p>Options for Q7</p> <ul style="list-style-type: none"> <li>a) Put documents, disks, other records containing personal information (including your purse) in a drawer or otherwise out of sight.</li> <li>b) Hit "control-alt-delete" and lock your computer.</li> <li>c) Call your best friend and have a long chat.</li> <li>d) Both a and b above.</li> </ul> <p>3.21.08 58</p>	
<p>Slide 59</p>	 <p>Correct Answer to Q7</p> <ul style="list-style-type: none"> <li>d) Both a and b above. <ul style="list-style-type: none"> <li>● Put documents, disks, other records containing personal information (including your purse) in a drawer or otherwise out of sight.</li> <li>● Hit "control-alt-delete" and lock your computer.</li> </ul> </li> </ul> <p>3.21.08 59</p>	<p>c) Both a and b above.</p> <p>Even when leaving your workstation temporarily during the day, lock your computer by ("control-alt-delete" and lock) to protect the data on it, and also put paper records, CDs, floppy disks, thumb drives and any other storage media away out of sight. When leaving for the day, shut down your computer and lock up all other data.</p>
<p>Slide 60</p>	 <p>Quiz Question 8</p> <p>● A state employee gives a printout of the names, addresses, and driver's license numbers of people who received unemployment benefits to a friend who wants to offer jobs to them. Which of the following are true?</p> <p>3.21.08 60</p>	

<p>Slide 61</p>	 <p>Options for Q8</p> <ul style="list-style-type: none"> <li>a) The employee may be found guilty of a misdemeanor punishable by up to \$5,000 and one year in jail.</li> <li>b) The employee may be fired.</li> <li>c) The employee's department may be sued.</li> <li>d) The employee will not be punished because his intentions were good.</li> </ul> <p>3.21.08 61</p>	
<p>Slide 62</p>	 <p>Correct Answer to Q8</p> <ul style="list-style-type: none"> <li>a) The employee may be found guilty of a misdemeanor punishable by up to \$5,000 and one year in jail.</li> <li>b) The employee may be fired.</li> <li>c) The employee's department may be sued.</li> </ul> <p>3.21.08 62</p>	<p>a), b), and c).</p> <p>The Information Practices Act contains penalties and consequences for those who violate it. Giving this kind of personal information to an unauthorized person places individuals at risk of identity theft, among other things.</p> <p>a) The employee may be found guilty of a misdemeanor punishable by up to \$5,000 and one year in jail as stated in Civil Code §1798.56. Any person who willfully requests or obtains any record containing personal information from an agency under false pretenses...</p> <p>b) The employee may be fire as stated in Civil Code §1798.55.</p> <p>c) The employee's department may be sued as stated in Civil Code § 1798.45.</p>

Slide  
63

The slide content is displayed within a yellow rectangular box with a black border. At the top of the box, there is a decorative header consisting of five small, horizontal rectangular segments in shades of blue, purple, and brown. The title "Privacy Resources" is centered at the top of the yellow area in a dark blue font. Below the title, there are three bullet points, each preceded by a small globe icon. The first bullet point is "California Privacy Laws" with a sub-bullet "Privacy Laws page at www.privacy.ca.gov". The second bullet point is "Consumer Information" with a sub-bullet "Consumers page at www.privacy.ca.gov". The third bullet point is "Identity Theft Information" with a sub-bullet "Identity Theft page at www.privacy.ca.gov". At the bottom left of the yellow box, the date "3.21.08" is printed in a small font. At the bottom right, the number "63" is printed in a small font. Below the yellow box, there is another decorative footer consisting of five small, horizontal rectangular segments in shades of blue, purple, and brown, matching the header.

**Privacy Resources**

- California Privacy Laws
  - Privacy Laws page at [www.privacy.ca.gov](http://www.privacy.ca.gov)
- Consumer Information
  - Consumers page at [www.privacy.ca.gov](http://www.privacy.ca.gov)
- Identity Theft Information
  - Identity Theft page at [www.privacy.ca.gov](http://www.privacy.ca.gov)

3.21.08 63